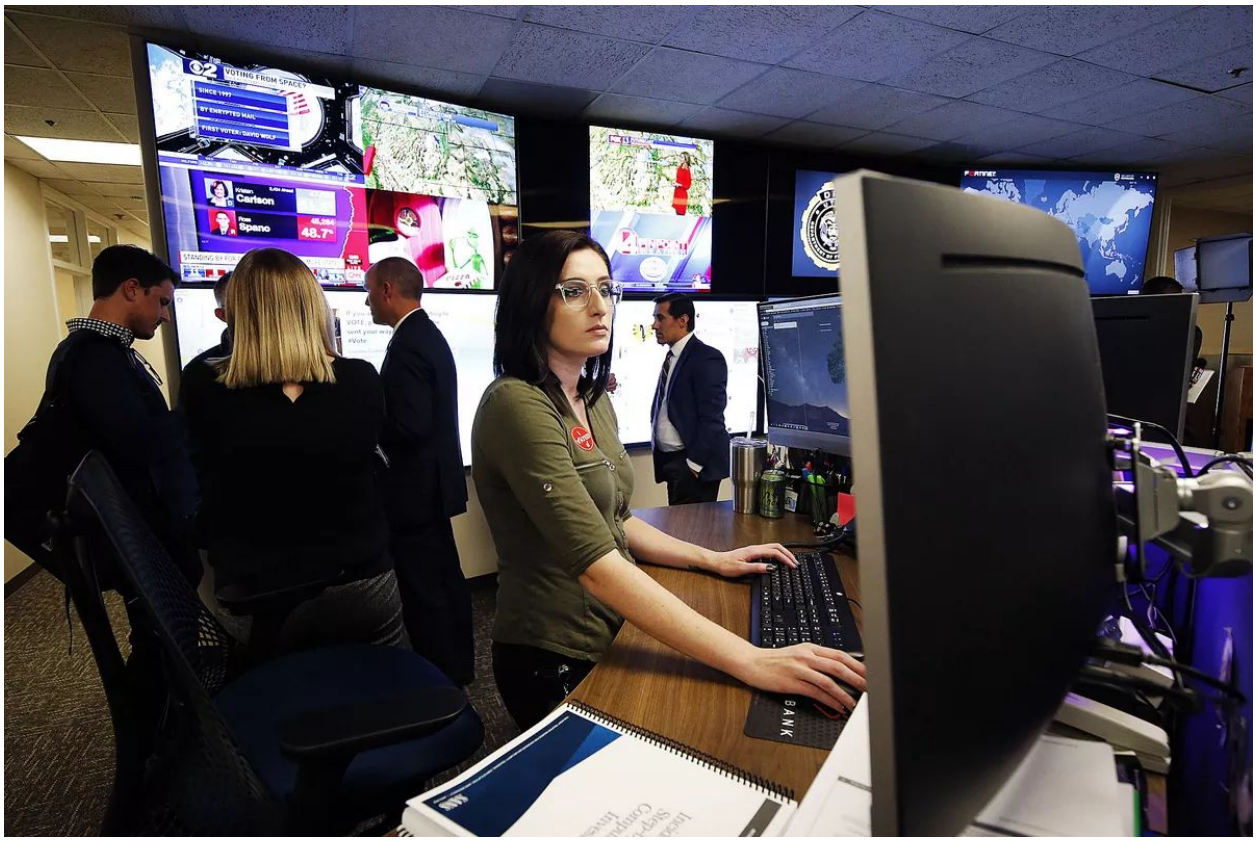
NASCIO 2020

1. Title: Utah Cyber Center
2. Category: Cyber Security
3. Project Initiation and Completion Date: January 2018 - May 2019
4. Project Contact: Phil Bates

Project Website: https://dts.utah.gov/security/security-services



Executive Summary

In July 2018, Utah's CIO announced the soft launch of the Utah Cyber Center with the goal of providing a more integrated approach to cybersecurity and response. Through coordination with the Attorney General, the Utah Department of Public Safety, the US Department of Homeland Security, and others, DTS created a system that brought together diverse stakeholders into a single operational center, providing a variety of coordinated resources. The Center was fully operational prior to the 2018 election in November (https://www.govtech.com/pcio/During-Election-Utahs-Cyber-Center-Wards-Off-Threats.html), a time when cyber attacks were expected to peak.

The realization of the Cyber Center has been particularly helpful in responding to a growing number of threats such as ransomware against targets such as local governments and small businesses who, on their own, do not have the resources to respond to those challenges. It also enables a 24x7 capability that can respond effectively to the digital threat environment facing the state. The Utah Association of Counties and the Utah League of Cities and Towns both encourage participation after having seen the benefits to their members of the Center who have saved hundreds of thousands of dollars through improved response to ransomware attacks.

Concept

The Utah Cyber Task Force was formed in 2013 as a joint effort between the Department of Public Safety (SIAC, SBI, DEM) and the Department of Technology Services (Enterprise Security) to develop teams that could respond to the ever-increasing Cyber Threat the state was dealing with.

Over the years the Federal Bureau of Investigations, Department of Homeland Security and other state agencies have added to the belief that we need to be prepared to address cybersecurity threats. These agencies have assumed responsibility to protect the people of Utah and the state's information assets.

There was a need to establish a central unified state interface for coordinating cybersecurity monitoring, sharing information, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among government agencies.

In 2018 the DTS repurposed space in the basement of the State Office Building at the Capitol into a temporary Cyber Center. The Cyber Center provides a central location for DTS, Public Safety, Attorney General's office, and other government employees to share intelligence and tactics, and respond to events in a more coordinated fashion.

The Cyber Center allows all known or suspected Cyber Security incidents to be reported to one single point of contact, disclosing all known information and interactions, immediately upon discovery. The Cyber Center is now the center point for Election Security coordination and monitoring.

Significance

The Utah Cyber Center opened in June 2018. The multi-agency facility is a joint effort of the Department of Technology Services, the Department of Public Safety, the Bureau of Criminal Investigations, the FBI, and the Department of Homeland Security. Other agencies participate on an as-needed basis. The Cyber Center also provides outreach to local government and private sector business. The Utah Cyber Center addresses a growing demand for expertise that can address a growing cyber threat environment after the state had observed a significant growth in attempted intrusions, denial of service attacks, and other types of cyber threats. Bot networks and other sophisticated attack vectors have increased the number of attempted cyber intrusions into the hundreds of millions.

The Cyber Center combines the best of trained personnel, advanced cyber response tools, and sophisticated analytics with access to external resources such as the Multi-State ISAC in a state that relies heavily on digital services to scale to its population. The Cyber Center uses geoblocking and other methods to reduce the attack surface when possible. Recently, the

Center has provided support for response to ransomware attacks against several counties and cities who often lack dedicated cyber response capabilities.

The Utah Cyber Center provides a physical location where all participants in the Utah Cyber Task Force, as well as others such as the Attorney General and local governments, can come together to more effectively respond to the growing cyber threat environment.

With help from intelligence analysts at DPS's Statewide Information and Analysis Center (SIAC) and technical experts from the state Department of Technology Services (DTS), DPS produces an analysis of the current climate for cyber crime, as well as predictions for the future growth of cyber crime. SIAC personnel have created a presentation predicting a proliferation of cyber crime.

In 2012, DPS asked for dedicated funding to staff two-full time cyber crime investigators in addition to a cyber crime analyst, and the legislature provided more than was requested by approving funding for three investigators and a civilian analyst. This helped form a foundation for the Cyber Crimes Task Force.

In Utah, a centralized IT department, the Department of Technology Services (DTS), protects all state agencies' various networks from breach. When DPS investigators are investigating cyber

attacks against Utah state agencies, it is much easier to work with one IT department on standardized networks. This centralization also facilitates dissemination of best practices and training of IT personnel.

In place of DTS's IT staff's past practice to wipe an affected network clean to remove the threat, following the creation of the Cyber Crimes Unit and emphasis on actively investigating cyber incidents, staff are now trained to properly preserve forensic digital evidence.

If there is cause to believe that a cyber crime has occurred, information is entered in the DPS's case tracker system for vetting by the cyber intelligence analyst and investigators to determine whether investigators will open a criminal case. Even if the evidence does not have a criminal nexus, there may still be an intelligence value; for example, a description of a tradecraft or technique that a particular cyber attacker employs that has not yet been seen in Utah. If there is intelligence value to the data, the cyber intelligence analyst determines whether it constitutes actionable intelligence and the best format (e.g., intelligence product) for dissemination among information sharing networks like the Utah State Cyber Intelligence Network. DTS is able to share information on the threat environment that is useful in tracking cyber criminals. Both DTS and DPS are able to draw on expertise from national experts such as the MS-ISAC.

For DPS investigators, partnering with the FBI had several important benefits that enabled the cyber unit to be effective: 1) the FBI provided the essential multi-jurisdictional reach needed to address cases where the victims or perpetrators were located outside of Utah; 2) the FBI provided hands-on training and mentorship for complicated technical skills; and 3) the FBI's database gave access to crucial information for vetting and investigating cases, as well as exploring potential associations among separate cyber incidents.

The relationship allows for crucial deconfliction of efforts. In some cases, a victim of a cyber crime might report to one or more of the following: their local police agency, the FBI, or IC3. Particularly because cyber crime investigations are so lengthy and extensive, it is crucial for agencies to share information to reduce redundant efforts.

Partnering with the FBI has enabled Utah's Cyber Crimes Unit to effectively address many cases due to the FBI's wide jurisdictional reach. It is rare that in either high-tech or computer-enabled crime, the perpetrator and the victim live in the same jurisdiction. Limiting the jurisdiction to the state of Utah in the first year of the Cyber Crimes Unit's existence severely hampered the team's ability to investigate many leads.

Partnering with the FBI is a promising practice that provides an answer to the multi-jurisdictional nature of cyber crime. Because of DPS's role as a state law enforcement agency, the department has strong relationships with local law enforcement agencies in Utah and other departments throughout the region. These relationships develop as investigators from different agencies work cases together. In some cases, cyber investigations have led to suspects or middlemen in a different part of the country.

Partnering with the FBI also provides other benefits to state investigators. State investigators are teamed with FBI agents who serve as mentors on cases with difficult technical issues. This hands-on aspect allows investigators to develop skills more quickly. Because state investigators complete a security clearance process, they are able to access FBI databases that contain a wealth of intelligence on cyber incidents.

In order to understand the threats facing the private sector, the Utah DPS is encouraging private-sector agencies to identify an employee who can participate in SIAC on a full-time basis. This employee will work with the cyber intelligence analyst in real time to analyze threats and enhance the state's cybersecurity network and response to attacks.

A ransomware attack hit Garfield County's computer systems in February 2019, crippling them for weeks before they were able to regain access to their own data.

"All of our data had been taken," Garfield County Attorney Barry Huntington said of the data breach. An employee had clicked on a phishing email earlier that launched a ransomware attack, locking up a number of county offices' data. The County Assessor's Office and the Recorder's Office had some of their data removed. Eventually the county received an email stating that terrorists had taken their information and if they wanted it, the county would have to pay them.

After the County reported the incident to the State Auditor who referred them to the Cyber Center, staff at the Center were able to work with the County to minimize the impact. The Utah Association of Counties shared the experience at their annual meeting and the Center is now working with other cities and counties to provide expertise that doesn't exist in most of those organizations.

References

URL(s): https://dts.utah.gov/security,
https://www.govtech.com/security/A-Place-for-Cyber-in-Utah.html,
https://www.govtech.com/pcio/During-Election-Utahs-Cyber-Center-Wards-Off-Threats.html,